Plec de prescripcions tècniques particulars que regeix la contractació basada relativa a la prestació d'un servei de suport a l'Agència de Ciberseguretat de Catalunya en l'elaboració de materials docents, estructurada en 1 lot

Exp. CB25AMCONSL1B022

Índex

1 Introducció

L'Agència de Ciberseguretat de Catalunya (en endavant, Agència), establerta sota el marc de la Llei 15/2017, del 25 de juliol, és l'entitat que lidera i coordina els esforços de la Generalitat de Catalunya en la protecció de la informació i les infraestructures del país davant les ciberamenaces. En un món digitalitzat i interconnectat, la seguretat de la informació s'ha convertit en una prioritat estratègica, i l'Agència subratlla el compromís de Catalunya amb la promoció d'un entorn digital segur i de confiança.

Amb un enfocament clar en la prevenció i detecció de ciberamenaces, la resposta efectiva davant incidents de ciberseguretat, la promoció de la cultura de ciberseguretat, i la col·laboració i coordinació amb diferents actors a nivell local i internacional, l'Agència opera dins de l'àmbit d'actuació definit per la llei, que marca les directrius d'actuació de l'Agència, les seves funcions, estructura orgànica i el règim de governança.

L'Agència sota la direcció estratègica del Govern de la Generalitat de Catalunya, en coordinació amb les entitats del sector públic de l'Administració de la Generalitat de Catalunya, i col·laborant amb governs locals de Catalunya, sector privat i societat civil és l'encarregada d'establir i de liderar el servei públic de ciberseguretat i té com a objectiu garantir una Societat de la Informació segura i confiable per al conjunt de la ciutadania catalana i de la seva Administració Pública, amb la voluntat d'esdevenir un referent a nivell nacional i internacional en matèria de ciberseguretat.

Els avenços impulsats per l'Estratègia 2019-2022 han establert un sòlid punt de partida per a futures accions, incloent la consolidació de l'Agència de Ciberseguretat com a entitat de referència. Aquests avenços no només han millorat la capacitat de resposta davant incidents sinó que també han promogut una major consciència i formació en ciberseguretat entre la ciutadania i les organitzacions. La nova Estratègia 2023-2027, "Una Catalunya Cibersegura en una Europa Digital", s'orienta cap a reforçar la resiliència digital, protegir els serveis i infraestructures essencials, i assegurar que ciutadans i organitzacions es beneficiïn de tecnologies digitals de confiança.

En el marc de l'activitat gestionada per l'Agència de Ciberseguretat, cal destacar que *segons recull la memòria de l'Agència de Ciberseguretat de Catalunya de 2023, l'entitat ha tingut un paper rellevant en les tasques de resposta i coordinació per a la gestió d'incidents de seguretat durant el 2023, tant pel que fa a la Generalitat com en diferents entitats del territori català.* En aquest sentit, l'Agència gestiona més de 2.200 sistemes d'informació, més de 220.000 usuaris i un perímetre de 24 departaments i organismes rellevants. Aquest perímetre protegit provoca un alt nivell d'activitat de gestió. Més concretament, el nombre de ciberatacs rebuts durant l'any 2023 va ser de més de 5.000 milions, en contraposició als 4.400 milions d'atacs del 2022. Pel que fa als incidents de seguretat, l'Agència en va gestionar prop de 2.670 durant el 2023, en comparació amb els 2.175 de l'exercici anterior.

Les xifres fan paleses la necessitat de dotar-se de noves eines i de seguir ampliant el perímetre d'actuació. En aquest sentit, i alineat amb la nova Estratègia, l'Agència ampliarà el seu perímetre d'actuació i per tant, incrementar el nivell de protecció, resiliència i prevenció de més àmbits.

Aquest contracte està finançat per Fons Europeus. El programa RETECH constitueix un dels nous eixos transversals de l'Agenda España Digital 2026 promoguts pel Ministerio de Asuntos Económicos y Transformación Digital, i està alineat amb dues de les principals fites de l'Agenda, com són, liderar la transformació digital de manera inclusiva i sostenible i focalitzar els esforços de digitalització en sectors econòmics clau. L'objectiu del Programa RETECH és impulsar xarxes territorials

d'especialització tecnològica, articulant projectes regionals que s'orientin a la transformació i especialització digital, assegurant la coordinació, la col·laboració i la complementarietat.

Gràcies a aquest nou eix de l'Agenda España Digital 2026, es pretén liderar un canvi disruptiu, de manera inclusiva i sostenible, focalitzant els esforços de digitalització en sectors econòmics clau. En definitiva, la iniciativa RETECH permetrà impulsar els projectes tractors proposats per les Comunitats i Ciutats Autònomes, fomentant l' intercanvi de coneixement i multiplicant les oportunitats de cada regió, a través de xarxes d' impacte nacional que permetin maximitzar l'equilibri territorial i la cohesió social entre elles.

Per fer efectiva la iniciativa RETECH amb total transparència i igualtat d'oportunitats per a totes les Comunitats i Ciutats Autònomes interessades, el Ministerio de Asuntos Económicos i Transformación Digital, a través de la Secretaria d'Estado de Digitalización e Inteligencia Artificial, va llançar una invitació pública destinada al desenvolupament de propostes de cooperació per finançar iniciatives emblemàtiques d'especialització territorial tecnològica dins de les seves competències.

2 Descripció dels serveis objecte de la contractació basada.

2.1 Context dels serveis objecte de la licitació.

Concretament s'emmarca en el:

Lot [1 Consultoria de ciberseguretat inclosa la vessant d'arquitectura]

Dins d'aquest lot s'inclouen [Tasques relacionades amb la formació a formadors i el desenvolupament d'ecosistema de Ciberseguretat:

- Alineament, desenvolupament, promoció i gestió d'itineraris formatius en ciberseguretat, fomentant la col·laboració amb la capacitació de professionals, el sector privat i altres administracions.
- Coordinació, promoció i execució d'iniciatives i activitats d'assistència tècnica i formatives per a la divulgació de la cultura de ciberseguretat, així com la creació i manteniment de kits per a mentories i temaris formatius en ciberseguretat.
- Desenvolupament, suport al desplegament, gestió i evolució de les comunitats i l'ecosistema de ciberseguretat, donant suport en la promoció d'esdeveniments i la participació de l'Agència i el sector de la ciberseguretat català en activitats i programes nacionals i internacionals.].

2.2 Objecte i abast dels serveis.

L'objecte de la present licitació és per a la prestació d'un servei de suport a l'Agència en l'elaboració de materials docents.

i. Objecte i descripció

L'objecte és la contractació d'un servei de suport a l'Agència en l'elaboració de materials docents tals com la gravació de materials didàctics i la impartició de classes en el marc del projecte de Ciberacadèmia de l'Agència de ciberseguretat de Catalunya (en endavant l'Agència). Aquests servei ha de proporcionar formació complementària a la prevista en format digital a la Ciberacadèmia.

La prestació del servei es farà en format B-learning, predominarà la modalitat participativa virtual (en línia), si bé es requerirà l'assistència física a l'espai formatiu previst per algunes gravacions (presencial) segons les necessitats del programa.

El servei no només contempla la realització de les tasques d'impartició de classes, gravació de continguts i avaluació, sinó que també actuaran, en una metodologia de formació guiada, com a figures de suport pedagògic (acompanyant els estudiants en la comprensió dels continguts digitalitzats, contribuint a reforçar-ne l'aprenentatge mitjançant sessions explicatives, resolent de dubtes o avaluant els coneixements adquirits).

Per a la realització de l'objecte del contracte l'adjudicatari haurà de poder disposar de diferents perfils professionals. Aquesta capacitació, estructurada segons la nomenclatura de perfils definida per l'European Cybersecurity Skills Framework (ECSF) de l'Agència europea ENISA, es desenvoluparà

mitjançant diferents itineraris formatius adaptats a les competències específiques de cada perfil i al seu nivell d'accés. A continuació, es detallen els perfils que conformen l'estructura formativa prevista:

1. Professional de proves de penetració (*Penetration Tester*)

   Aprendre a fer proves de penetració per identificar vulnerabilitats en els sistemes de l'organització i proposar solucions per corregir-les.

2. Auditor/a de ciberseguretat (*Cybersecurity Auditor*)

   Conèixer com fer auditories per verificar el compliment de les polítiques de seguretat i identificar àrees de millora.

3. Cap de seguretat de la informació CISO (*Chief Information Security Officer*)

   Quins rols i funcions han de desenvolupar-se com a responsable de la seguretat de la informació dins una organització, definir polítiques de seguretat, supervisar el compliment i gestionar incidents de ciberseguretat.

4. Consultor/a d'equips de resposta a incidents (*Cyber Incident Responder*)

   Aprendre a gestionar i respondre els incidents de seguretat, minimitzant l'impacte i recuperant la normalitat operativa.

5. Expert/a en ciberseguretat legal (*Cyber Legal, Policy & Compliance Officer*)

   Saber com fer que una organització compleixi amb les regulacions i estàndards de seguretat, desenvolupant polítiques i proporcionant assessorament legal.

6. Expert/a en intel·ligència d'amenaces (*Cyber Threat Intelligence Specialist*)

   Saber analitzar i interpretar informació sobre amenaces cibernètiques per anticipar-se a possibles atacs i millorar les defenses de l'organització.

7. Arquitecte/a de ciberseguretat (*Cybersecurity Architect*)

   Aprendre a dissenyar l'arquitectura de seguretat d'una organització, integrant solucions tecnològiques per protegir les dades.

8. Educador/a de la ciberseguretat (*Cybersecurity Educator*)

   Saber com desenvolupar i impartir programes de formació i conscienciació en seguretat per capacitar els empleats en pràctiques segures.

9. Expert/a en la implementació de la ciberseguretat (*Cybersecurity Implementer*)

   Ha d'aprendre a implementar solucions de seguretat en els sistemes de l'organització, i garantir la protecció contra amenaces.

10. Expert/a en gestió de riscos (*Cybersecurity Risk Manager*)

    Ha de saber avaluar els riscos de seguretat i proposar mesures per mitigar-los, garantint la protecció dels actius de l'organització.

11. Investigador/a forense digital (*Digital Forensics Investigator*)

    Ha d'aprendre a realitzar metodologia d'anàlisis forenses per investigar incidents de seguretat, a recopilar i a preservar proves digitals.

ii. Objectius del servei

Els objectius del servei són garantir una formació de qualitat orientada al desenvolupament de competències específiques per a cada perfil professional vinculat a l'àmbit de la ciberseguretat.

Aquesta servei ha d'estar realitzat per professionals especialitzats i estructurada de manera coherent i progressiva, d'acord amb els mòduls i nivells definits en el marc de la Ciberacadèmia. A més de la impartició de sessions formatives, el servei inclou la generació de materials didàctics multimèdia que expliquin els continguts del programa de manera clara, estructurada i comprensible, amb l'objectiu de facilitar l'autonomia de l'estudiant i afavorir l'aprenentatge asíncron.

El servei també ha de garantir un suport pedagògic continuat durant tot el procés formatiu, que inclogui la resolució de consultes, l'orientació individualitzada i el foment de la participació activa dels estudiants. Així mateix, s'haurà de dur a terme l'avaluació dels aprenentatges de l'alumnat, d'acord amb els criteris i instruments establerts per la Ciberacadèmia, amb l'objectiu de verificar l'assoliment dels objectius formatius i contribuir a la millora contínua del procés d'ensenyament-aprenentatge.

iii. Activitats i funcionalitats que s'esperen del servei

El servei implicarà un conjunt d'activitats orientades a assegurar la qualitat de la formació i l'adequació pedagògica dels continguts. En primer lloc, els responsables de l'execució del contracte seran els responsables de la gravació de materials didàctics audiovisuals, com vídeos explicatius i tutorials, que serviran com a base formativa per a l'estudiant.

També es preveu la realització de sessions formatives en línia, ja siguin síncrones o asíncrones, amb l'objectiu de reforçar els continguts i fomentar la interacció.

S'haurà de facilitar el suport pedagògic necessari, resolent dubtes i aprofundint en els aspectes més complexos dels temaris. D'altra banda, supervisaran i dinamitzaran hores de laboratori o altres activitats pràctiques, afavorint l'aplicació real dels coneixements adquirits.

Finalment, participaran en l'avaluació del progrés dels estudiants i proporcionaran feedback constructiu per millorar-ne el rendiment acadèmic i professional.

iv. Productes del servei

Els productes derivats del servei hauran de cobrir les necessitats formatives dels diferents itineraris, oferint una experiència d'aprenentatge integral i coherent. Entre aquests productes s'inclouen els materials didàctics gravats, que consistiran en vídeos explicatius i tutorials dissenyats per facilitar la comprensió autònoma dels continguts. També es generaran sessions de formació en línia, tant en directe com enregistrades, orientades a complementar els materials digitalitzats. A més, es preveu la creació de materials de suport, com guies d'estudi, exercicis pràctics i altres recursos com informes d'avaluació que recullin el progrés dels estudiants i determinin l'assoliment del contingut impartit.

Atès que el servei es presta en modalitat B-learning i predominantment en línia, els materials docents audiovisuals generats en el marc del contracte hauran de ser funcionals, reutilitzables i integrables en l'entorn digital de formació utilitzat per l'Agència.

L'empresa adjudicatària serà responsable de garantir que els materials lliurats permeten la seva correcta integració, visualització, ús pedagògic i reutilització en aquest entorn. Els materials que no compleixin aquests requisits no es consideraran lliurats correctament a efectes de validació del servei.

Les activitats pràctiques supervisades, com les sessions de laboratori i les pràctiques en entorns de simulació tipus *CiberRange*, completaran l'experiència formativa, permetent la posada en pràctica dels coneixements en entorns controlats i guiats per professionals especialitzats. Aquestes activitats facilitaran l'adquisició de competències tècniques mitjançant la resolució de casos reals i escenaris simulats, afavorint un aprenentatge aplicat i contextualitzat.

2.3 Característiques del servei.

D'acord amb l'objecte del contracte i per a la correcta execució del servei, s'estableixen a continuació els elements essencials que han de regir la prestació del servei:

Configuració del servei

Els perfils del servei hauran de ser professionals especialitzats en ciberseguretat, amb un coneixement profund dels continguts associats a cada itinerari formatiu i amb capacitat pedagògica per transmetre'ls de manera clara, estructurada i entenedora.

L'adjudicatari haurà d'aportar un nombre de perfils professionals suficient per garantir que podran complir amb el nombre totals d'hores assignades en el moment que el servei ho requereixi.

El personal adscrits al servei haurà de dominar el català, ja que aquesta serà la llengua vehicular de tots els materials i sessions formatives i hauran de poder atendre eventuals requeriments de presencialitat, segons les necessitats detectades pel coordinador acadèmic.

Participació i gestió del servei de formació

La participació dels professionals del servei s'articularà sota la direcció d'un coordinador acadèmic, figura clau per vetllar per la qualitat pedagògica i la coherència del conjunt de la formació. Serà aquest coordinador qui determinarà, en cada cas, si cal gravar un vídeo, si una sessió s'ha de fer en directe o presencial, o si certs continguts s'han de treballar en el marc de les hores de laboratori. En aquest sentit, s'haurà de garantir una adequada disponibilitat i capacitat d'adaptació dels professionals a les directrius d'aquest perfil.

L'empresa adjudicataria haurà de disposar d'una figura de coordinador/a de docència, responsable de la gestió integral de la bossa d'hores, qui assumirà les funcions següents:

- Assignació i coordinació dels professionals del servei.
- Coordinació directa amb el coordinador acadèmic.
- Seguiment de l'execució docent.
- Gestió administrativa i logística associada a la docència.

Aquesta figura gestionarà una bossa global d'hores destinades al servei dins el marc de la Ciberacadèmia, assegurant el control i seguiment constant de les hores consumides, assignades i disponibles. També garantirà que totes les sessions formatives programades disposin d'un professional assignat, coordinant tant les eventuals modalitats presencials com les sessions gravades, i vetllant per l'adequació del perfil dels formadors a cada contingut. Treballarà estretament amb el coordinador acadèmic per organitzar la cobertura de totes les activitats formatives, supervisarà l'execució de les sessions planificades i gestionarà els aspectes logístics i administratius vinculats a la participació del personal docent.

Disponibilitat

Atesa la naturalesa flexible del servei, i el fet que l'activació efectiva de les hores de docència estarà supeditada a la definició progressiva dels itineraris formatius, calendaris i sessions de la Ciberacadèmia, l'empresa adjudicatària haurà de disposar d'una capacitat operativa suficient per garantir la disponibilitat de l'equip docent d'acord amb la planificació que es derivi del servei de la Ciberacadèmia.

Aquesta capacitat haurà de permetre donar resposta a les necessitats de gravació de continguts, impartició de sessions formatives i avaluació de l'alumnat durant el període d'inici i desplegament dels itineraris, sense que sigui exigible una planificació prèvia tancada. Per tant, el servei haurà de mantenir un marge de flexibilitat suficient per adaptar-se a l'activació exponencial i progressiva del projecte.

Per tal de facilitar una correcta estimació dels recursos d'equip docent necessaris per part de l'adjudicatari, s'adjunta a continuació un quadre amb el nombre d'hores aproximades assignades a cada formació i mòdul formatiu. Cal tenir en compte que el nombre total d'hores de formació indicades no equival al total d'hores de docència directa que s'impartiran, ja que una part d'aquestes hores corresponen a treball autònom de l'alumnat, sense intervenció directa del personal docent.

Matèria de ciberseguretat / correspondència d'hores previstes per perfils ciber	CISO	LEGAL	EDUCADOR	AUDITOR	RISC	INTEL·LIGÈNCIA	PENTESTER	ARQUITECTE	IMPLEMENTADOR	INCIDENTS	FORENSICS
Fonaments de la ciberseguretat	22	15	15	22	22	15	15	22	15	15	15
Seguretat de les aplicacions	2	-	-	-	-	2	6	6	8	4	2
Identitat Digital	4	2	-	2	-	4	6	4	4	4	2
Protecció i privacitat de dades	11	22	-	17	17	6	-	11	11	6	6
Ciberdefensa	12	-	-	-	-	38	38	12	4	38	38
Estructura organitzativa i processos empresarials	2	2	2	2	2	1	1	2	1	1	1
Habilitats interpersonals (*soft skills*)	3	2	1	2	2	1	1	3	1	1	1
TOTAL D'HORES	56	43	18	45	43	67	67	60	44	69	65

Així mateix, cal tenir en compte que el còmput d'hores previstes dins del servei es farà en base a hores efectives de docència impartida o productes lliurats (com ara vídeos gravats o sessions realitzades), i no en funció del temps de preparació o dedicació interna que aquestes activitats puguin haver requerit. Aquesta consideració és clau per assegurar un ús eficient de la bossa d'hores disponible i garantir la màxima rendibilitat i impacte formatiu del servei.

Revocació dels professionals tècnics

Per últim, l'Agència es reserva el dret de revocar la participació d'un professional tècnic proposat per l'empresa adjudicatària en qualsevol moment de l'execució del contracte, en els següents supòsits:

1. Incompliment dels requisits tècnics o formatius establerts en els plecs o en la proposta presentada.
2. Valoracions negatives reiterades per part de l'alumnat o de la coordinació acadèmica, especialment en relació amb la qualitat pedagògica, el nivell tècnic o la capacitat comunicativa.
3. Falta d'adaptació als continguts o metodologia establerts per la ciberacadèmia.
4. Inassistència injustificada o reiterada impuntualitat a les sessions formatives.
5. Incompliment de les normes de convivència, respecte o confidencialitat establertes per l'organització.

En cas de revocació, l'empresa adjudicatària haurà de proposar un/a nou/va docent en un termini màxim de 5 dies naturals, que haurà de ser validat per l'òrgan contractant. El nou perfil haurà de complir com a mínim amb els mateixos requisits que el docent substituït.

3 Condicions d'execució del servei

3.1 Horaris

El servei s'haurà de prestar d'acord amb els horaris de prestació dels serveis de l'Agència, 8x5 en horari de dies laborables. Es considera horari de dies laborables els dies que siguin laborables al centre de treball de l'Hospitalet de Llobregat amb prestació de 9:00h a 18:00h.

A petició expressa de l'Agència, es podria demanar la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei.

Si durant l'execució del contracte l'Agència o l'adjudicatari detecten la necessitat de modificar l'horari del servei o equip descrit en aquest plec, l'Agència i l'adjudicatari consensuaran de forma conjunta la modificació, essent l'Agència qui finalment designi l'horari de prestació que s'adeqüi a les necessitats pròpies i que no perjudiqui de forma excessiva a l'adjudicatari.

3.2 Localització física.

Inicialment, els equips prestataris dels serveis estaran ubicats físicament a les oficines de l'adjudicatari o en alguna altra que ambdues parts acordin, atenent sempre a la seguretat de la informació gestionada pel servei. Tot i això, l'Agència considera que l'adjudicatari, en coordinació amb la Direcció de l'àrea de l'Agència, podria arribar a prestar/executar fins al 50% de les tasques/projectes/serveis amb recursos ubicats a les instal·lacions de l'Agència de Ciberseguretat a l'Hospitalet de Llobregat.

La prestació del servei es farà en format B-learning, predominarà la modalitat participativa virtual (en línia), si bé es requerirà l'assistència física a l'espai formatiu previst per algunes gravacions (presencial) segons les necessitats del programa.

Al llarg del contracte es podria requerir un canvi en la ubicació dels professionals, d'acord amb les necessitats dels serveis i l'organització d'equips de treball. En cap cas la ubicació dels professionals suposarà un increment dels costos vinculats a la prestació dels serveis.

En coherència amb aquests requeriments, i tal com s'ha establert prèviament en el plec, es valorarà positivament que els equips estiguin ubicats en el territori, amb l'objectiu de facilitar una resposta eficient a eventuals requeriments de presencialitat o a la realització de sessions en directe, segons les necessitats que pugui determinar el coordinador acadèmic.

3.3 Equip de treball

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos de l'adjudicatari del contracte basat amb la qualificació necessària i adequada per a la prestació del servei.

Els mitjans personals necessaris per a la prestació dels serveis han de ser els adequats per realitzar amb garantia les tasques definides i han de mostrar les habilitats necessàries per tal d'integrar-se en un equip d'alt rendiment, entre les quals es podrien determinar a efectes enunciatius les següents:

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.
- Destresa comunicativa i interpersonal.
- Capacitat de treballar en equip.
- Habilitat per identificar, analitzar i resoldre problemes.
- Coneixement de català, castellà i d'anglès, parlat i escrit.
- Ampli coneixement legal, tecnològic i de negoci de seguretat informàtica i de l'entorn de l'administració pública.
- Altres necessaris per al bon desenvolupament dels serveis.

L'adjudicatari haurà de disposar d'un equip de treball amb els perfils, dedicació i pla de treball adequats per a l'execució dels serveis sol·licitats en el present plec, d'acord amb les condicions i paràmetres esmentats en els apartats d'aquest plec.

No es preveu la possibilitat de transferència del personal intern de l'Agència o dels seus clients.

L'adjudicatari disposarà d'una figura que assumirà les tasques de **Coordinador/a de docència.** A aquest efecte, ha de assumir les següents responsabilitats:

1. **Gestió de la bossa d'hores:** El coordinador/a de docència serà responsable de gestionar una bossa global de les hores destinades a la impartició de classes dins el marc de la Ciberacadèmia. Aquesta gestió inclourà el control i seguiment constant de les hores consumides, les hores assignades i les hores disponibles, mantenint un registre actualitzat que permeti una visió clara i precisa de l'estat de la bossa docent en tot moment.
2. **Assignació i coordinació del personal docent:** Correspondrà a aquesta figura la tasca de garantir que totes les sessions formatives programades disposin d'un professional assignat. Per a això, haurà d'identificar, contactar i coordinar els professionals que impartiran les diferents sessions, tenint en compte tant les modalitats presencials com les sessions gravades. Així mateix, haurà de vetllar per l'adequació del perfil dels formadors a cada contingut, així com per la seva disponibilitat i compromís amb el calendari establert.

3. **Coordinació amb el coordinador acadèmic:** El coordinador/a de docència treballarà estretament amb el coordinador acadèmic, que serà l'encarregat de definir els continguts de cada curs, establir quines sessions s'impartiran i quines es gravaran, i determinar la planificació acadèmica global. A partir d'aquesta informació, el coordinador de docència haurà d'organitzar la cobertura de totes les activitats formatives, assegurant que es disposi del personal necessari per dur-les a terme amb garanties.
4. **Seguiment de l'execució docent:** Aquesta figura haurà de supervisar que les sessions planificades s'executin conforme al calendari i condicions previstes, i actuar amb rapidesa davant de qualsevol incidència, baixa o imprevist que pugui afectar la prestació del servei. També s'encarregarà de confirmar que les sessions gravades es duguin a terme correctament, segons les instruccions acordades i amb el nivell de qualitat requerit.
5. **Gestió administrativa i logística associada a la docència:** El coordinador/a de docència haurà de gestionar els aspectes logístics i administratius vinculats a la participació del personal docent, incloent-hi la preparació i comunicació dels horaris, la interlocució directa amb els formadors per a qüestions organitzatives i, si escau, la tramitació de la documentació necessària per a la seva contractació o col·laboració.

L'adjudicatari haurà de disposar d'un organigrama i d'esquemes d'equip que permetin donar resposta a les necessitats expressades en aquest plec, i els haurà de mantenir actualitzats durant l'execució del contracte.

Per raons d'operativitat, de coneixement de les tasques a realitzar i de sensibilitat de la informació amb la que es treballa, cal garantir al màxim la continuïtat de l'equip que donen servei a l'Agència.

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de **980 hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	Unitats estimades en hores
Perfil Coordinador/a de docència	**45 hores**
Perfils tècnics de ciberseguretat	**935 Hores**

Els requisits anteriors s'han d'entendre com a mínims aproximats, podent ser ampliats i millorats en les ofertes.

3.3.1 Perfils

Els requeriments mínims dels perfils professionals que poden composar l'equip són els següents:

PERFIL	REQUISITS
Coordinador/a docència	**Formació acadèmica:** • Graduat/ada universitari/ària (anteriorment diplomatures o llicenciatures). **Experiència:** • Acreditació d'un mínim de **tres anys d'experiència** en la coordinació o gestió de programes de formació, especialment en contextos d'educació per a adults, formació contínua o formació tècnica especialitzada. • Experiència en responsabilitats relacionades amb la planificació de cursos, l'assignació de docents, la gestió de calendaris i el seguiment de l'execució de l'activitat formativa. **Competències tècniques**: • Capacitat per treballar en equip, coordinar-se amb altres figures del projecte (com ara el coordinador acadèmic), comunicar-se amb l'equip de professionals, interlocutors diversos i resoldre incidències amb proactivitat i autonomia. • Domini d'eines digitals habituals per a la gestió de la formació (fulls de càlcul, eines col·laboratives i calendaris digitals). Es valorarà l'experiència amb plataformes de gestió de l'aprenentatge (LMS) i sistemes de seguiment docent. • Nivell C1 de català.

a) Perfils tècnics mínims de ciberseguretat

Els perfils tècnics que poden ser requerits per a l'execució del contracte inclouen:

1. Professional de proves de penetració (*Penetration Tester*)

   Aprendre a fer proves de penetració per identificar vulnerabilitats en els sistemes de l'organització i proposar solucions per corregir-les.

2. Auditor/a de ciberseguretat (*Cybersecurity Auditor*)

   Conèixer com fer auditories per verificar el compliment de les polítiques de seguretat i identificar àrees de millora.

3. Cap de seguretat de la informació CISO (*Chief Information Security Officer*)

   Quins rols i funcions han de desenvolupar-se com a responsable de la seguretat de la informació dins una organització, definir polítiques de seguretat, supervisar el compliment i gestionar incidents de ciberseguretat.

4. Consultor/a d'equips de resposta a incidents (*Cyber Incident Responder*)

   Aprendre a gestionar i respondre els incidents de seguretat, minimitzant l'impacte i recuperant la normalitat operativa.

5. Expert/a en ciberseguretat legal (*Cyber Legal, Policy & Compliance Officer*)

   Saber com fer que una organització compleixi amb les regulacions i estàndards de seguretat, desenvolupant polítiques i proporcionant assessorament legal.

6. Expert/a en intel·ligència d'amenaces (*Cyber Threat Intelligence Specialist*)

Saber analitzar i interpretar informació sobre amenaces cibernètiques per anticipar-se a possibles atacs i millorar les defenses de l'organització.

7. Arquitecte/a de ciberseguretat (*Cybersecurity Architect*)

   Aprendre a dissenyar l'arquitectura de seguretat d'una organització, integrant solucions tecnològiques per protegir les dades.

8. Educador/a de la ciberseguretat (*Cybersecurity Educator*)

   Saber com desenvolupar i impartir programes de formació i conscienciació en seguretat per capacitar els empleats en pràctiques segures.

9. Expert/a en la implementació de la ciberseguretat (*Cybersecurity Implementer*)

   Ha d'aprendre a implementar solucions de seguretat en els sistemes de l'organització, i garantir la protecció contra amenaces.

10. Expert/a en gestió de riscos (*Cybersecurity Risk Manager*)

    Ha de saber avaluar els riscos de seguretat i proposar mesures per mitigar-los, garantint la protecció dels actius de l'organització.

11. Investigador/a forense digital (*Digital Forensics Investigator*)

    Ha d'aprendre a realitzar metodologia d'anàlisis forenses per investigar incidents de seguretat, a recopilar i a preservar proves digitals.

Cada perfil tècnic mínim haurà de disposar de formació universitària o equivalent en l'àmbit TIC, coneixements acreditats en ciberseguretat avançada i participació substancial en l'objecte del contracte.

S'entén que aquests perfils es corresponen amb els rols que, des de l'Agència, s'identifiquen per la prestació d'aquest servei, deixant a la banda del l'adjudicatari la proposta de desplegament, composició de l'equip, adequació de perfils i dedicació global dels mateixos.

3.4 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari del contracte basat el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present apartat o per tal de garantir la correcta prestació, dimensionament i organització dels serveis. Aquesta substitució s'haurà de fer efectiva en el termini de 15 dies laborables a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència a l'empresa adjudicatària del contracte basat. L'adjudicatari haurà de presentar en un termini màxim de 10 dies laborables a partir de la comunicació de sol·licitud de substitució, el pla d'acció previst per resoldre les causes que han determinat la sol·licitud de substitució. Si l'objecte del contracte basat ho requereix, aquest aspecte es podrà concretar en aquest.

3.5 Control de rotació

L'estabilitat dels recursos del servei amb coneixement i compromís és molt important per a la correcta prestació del servei.

L'empresa adjudicatària del contracte basat podrà fer canvis en l'equip de treball durant l'execució del contracte, però ho haurà de notificar per escrit a l'Agència amb una antelació mínima de 14 dies naturals, justificant el canvi i informant del perfil i característiques de la persona que s'incorpora.

L'Agència comprovarà que la persona a incorporar compleix amb les condicions curriculars del component de l'equip que substitueixi.

L'empresa assumirà la selecció de les persones de nova incorporació, la coexistència en el servei del personal sortint i l'entrant sense cost per l'Agència, assegurant el correcte traspàs de coneixement en els següents 15 dies i duent a terme els controls necessaris per garantir-lo entenent, per tant, la no facturació d'aquests dies d'adaptació i traspàs. Sens perjudici que si s'escau es puguin aplicar els ANS corresponents per rotació excessiva.

En cap cas la substitució de personal suposarà un cost addicional, havent-se de garantir que el servei no es vegi afectat per aquest canvi. Si l'objecte del contracte basat ho requereix, aquest aspecte es podrà concretar en el contracte basat.

3.6 Eines i equipament per a la prestació de serveis.

Les principals eines requerides (gestió d'esdeveniments, alertes, sistema de registre, anàlisi de codi, web i infraestructura) per la prestació del servei seran proporcionades per l'Agència. L'empresa adjudicataria haurà de fer servir aquestes eines, no podent extreure informació fora de l'àmbit d'actuació per la seva manipulació o explotació sense autorització prèvia de l'Agència.

Quan l'adjudicatari es trobi en les instal·lacions de l'Agència, proveirà a les persones que prestin els serveis:

- Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de l'Agència.
- Infraestructura per al suport de les eines corporatives (servidors) i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides l'Agència.
- Telefonia fixa a les instal·lacions del servei.
- Telefonia mòbil per donar cobertura als serveis de guàrdia.
- Accés a Internet a través de la xarxa d'àrea local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.

L'Agència no proveirà:

- Ordinadors de sobretaula amb sistema operatiu i programari habitual d'oficina ni tampoc ordinadors portàtils amb el programari habitual de l'Agència.
- Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'Agència.
- Accés a Internet via GPRS, UMTS.
- Cap altre recurs no especificat explícitament.

En conseqüència, els adjudicataris hauran de:

- Subministrar tots elements de maquinari, programari i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments de l'objecte del contracte. Aquests elements seran *d'ús exclusiu* pels serveis prestats a l'Agència i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.
- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat Corporativa de l'Agència.

- Permetre l'administració, maquetat, esborrat i supervisió dels equips per part de l'equip de Mitjans Tècnics de l'Agència.

L'Agència es troba en un procés de revisió i millora contínua que pot implicar la realització de canvis importants en el referent a les eines que s'hauran d'utilitzar per dur a terme l'execució del servei.

Per aquest motiu és imprescindible que l'adjudicatari tingui presents les següents consideracions en el referent a les eines de gestió durant l'execució del contracte.

- L'Agència decidirà la utilització de qualsevol tecnologia nova o evolució de les existents, relacionades amb la prestació del servei.
- L'Agència decidirà la forma d'implantar qualsevol d'aquests nous sistemes, planificar els projectes corresponents i el seu calendari, així com la transició des dels sistemes existents cap als nous.
- Els adjudicataris es comprometen a assumir i adaptar-se a aquestes noves tecnologies i sistemes per donar el servei de suport, així com participar activament en el procés de transició, formant i preparant el seu personal en aquestes noves tecnologies i sistemes implantats sense cost addicional per l'Agència.

L'empresa adjudicatària haurà de disposar dels mitjans tècnics necessaris per a la producció, gravació, edició bàsica i lliurament dels materials docents audiovisuals objecte del contracte.

L'Agència podrà facilitar, si escau, espais físics per a la realització d'algunes gravacions presencials, sense que això comporti l'obligació de proporcionar equipament tècnic de gravació.

3.7 Gestió del coneixement

Amb l'objectiu de garantir que l'Agència disposi del coneixement necessari per a la correcta execució de les seves funcions com a Centre d'Innovació i Competència en Ciberseguretat (CIC4Cyber) i, especialment, l'impuls de la transformació fonamentada en el coneixement col·laboratiu, la coordinació de l'ecosistema de ciberseguretat i la voluntat per la innovació continua, es requereix que l'empresa adjudicatària registri tot el coneixement que disposi i es generi en la contractació basada que derivi del present Acord Marc d'acord amb les directrius del CIC4Cyber.

A tal efecte, l'adjudicatària haurà de mantenir aquest coneixement actualitzat i accessible per a l'organització, havent de proporcionar una descripció detallada del coneixement que es disposi i es generi al servei ofert, i tenint, per part de l'organització, accés a aquest coneixement en qualsevol moment.

3.8 Seguretat Corporativa

Un cop adjudicat el contracte basat, tant l'empresa adjudicatària com el personal de l'empresa adjudicatària s'haurà de sotmetre a les polítiques i regulacions internes que estableix l'àrea de Seguretat Corporativa en matèria de seguretat de la informació, com a mínim i no limitant-se a:

- Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per Seguretat Corporativa, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.
- Facilitar l'accés en excepcionalment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines de l'Agència (sigui o no per l'exercici de la seva funció).

- Acceptar les normes i polítiques que estableix l'àrea de Seguretat Corporativa tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.
- Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de l'àrea de Mitjans Tècnics per fer el desplegament de polítiques i controls de seguretat, actualització d'eines i manteniment d'aplicacions autoritzades i permisos d'accés a la informació.
- Els equips, així com la informació resident dels mateixos serà sempre custodiada per l'Agència.
- Garantir l'estabilitat dels equips (reduint al mínim la rotació de personal).
- Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (ENS, LOPDGDD, GDPR, LSSI, etc.).

A la finalització del contracte, l'adjudicatari del contracte basat quedarà obligat al lliurament o destrucció en cas de ser sol·licitada, de qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei.

3.9 Control de Gestió

L'empresa adjudicatària del contracte basat, i en especial el cap de servei, haurà de col·laborar amb el responsable de la planificació pressupostària i el control de gestió de l'Agència per tal:

- De complir amb el model de seguiment econòmic i planificació en termes de capacitat i execució de tasques.
- D'ajustar-se als procediments de facturació que determini l'Agència.
- De conformar les factures en relació amb el reportat de serveis efectuat i acceptat per l'Agència, d'acord amb els procediments establerts.
- D'exercir la gestió del contracte amb capacitats de *forecast.*
- Realitzar el *reporting* en les eines proporcionades per l'Agència amb els següents conceptes:
    - Fitxer mestre de persones.
    - Fitxer mestre de projectes i activitats.
    - Estimació de recursos per projecte.
    - Seguiment dels riscos.
    - Seguiment del consum de recursos.
    - Imputació de temps i activitats.
    - Assignació de tasques a persones.
    - Memòria d'activitat del contracte.
    - Facturació i Conformació de factures.

L'adjudicatari proporcionarà la seva total col·laboració per a la realització d'auditories i la verificació del compliment dels compromisos. Aquestes auditories, realitzades en qualsevol de les instal·lacions involucrades en la prestació del servei, podran ser portades a terme per personal de l'Agència o sol·licitades a tercers. No serà necessari fer una notificació prèvia per a la realització de tasques d'auditoria que no requereixin la col·laboració activa per part del personal de l'adjudicatari. En el cas

en què sigui necessària aquesta col·laboració, l'Agència farà una notificació amb dues setmanes d'antelació.

3.10 Documentació.

L'Agència és el propietari de tota la documentació elaborada pels adjudicataris referent al servei prestat pels adjudicataris i el seu personal i subcontractats que destini a l'execució dels serveis. L'adjudicatari s'encarregarà de disposar de totes les autoritzacions i permisos necessaris per tal de poder donar compliment a aquesta previsió, essent responsabilitat de l'adjudicatari qualsevol pagament o reclamació relativa a aquesta manca d'autoritzacions.

Els responsable de servei de l'Agència serà els responsable de la validació i aprovació dels documents elaborats pel personal de l'adjudicatari. En cas que la qualitat dels documents sigui molt baixa o de manera recurrent i/o perllongada en el temps de prestació dels serveis no assoleixi els nivells requerits s'aplicaran les penalitzacions establertes en la present licitació.

L'adjudicatari haurà de mantenir la documentació actualitzada en el sistema de gestió documental que l'Agència proporcioni per tal efecte

3.11 Formació

El personal de l'empresa adjudicatària del contracte basat realitzarà, si s'escau, formació continuada per tal de garantir l'actualització dels seus coneixements així com l'adquisició de nou coneixement que pugui ser de valor pels serveis de l'Agència.

3.12 Contingència

L'adjudicatari haurà de proveir un pla de contingència, en cas de desastre de les instal·lacions principals, en unes instal·lacions alternatives (centre de gestió secundari) propietat de l'adjudicatari, que inclouran:

- Estacions de treball amb el programari adequat per realitzar les tasques descrites.
- Comunicacions d'accés a les aplicacions informàtiques.
- Telefonia fixa a les instal·lacions del servei.
- Accés a Internet a través de la xarxa d'àrea local.
- Espai suficient per allotjar en condicions de treball òptimes:
    - El personal necessari de l'adjudicatari per realitzar el servei i
    - Personal de l'Agència, o de terceres parts determinades per aquest, per a la correcta gestió del servei.
- Pla i execució de proves per validar la solució de contingència implementada, amb la periodicitat que l'Agència determini.

Les instal·lacions i equipament haurà de ser suficient per garantir la continuïtat dels serveis de l'Agència durant l'existència de la causa que doni lloc a la contingència.

3.13 Metodologia, estàndards i lliurables

L'organització del treball i execució del servei s'haurà d'adequar a les metodologies, estàndards i lliurables establerts per l'Agència vigents en el moment de l'execució del servei objecte del contracte basat.

3.14 Seguretat

En matèria de seguretat de la informació, l'empresa adjudicatària té les següents obligacions:

3.14.1 Deure de confidencialitat

Tot el personal de l'empresa adjudicatària així com els possibles subcontractistes han de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels serveis contractats. Aquesta obligació de confidencialitat s'haurà de mantenir durant 10 anys, o el que s'especifiqui en el contracte basat, des de que es va tenir coneixement de la informació, excepte en relació a les dades personals a les que accedeixin respecte a les que caldrà mantenir el deure de confidencialitat de manera indefinida, subsistint inclús quan es finalitzi la relació contractual, segons estableix la Llei Orgànica 3/2018.

L'empresa ha de comunicar aquesta obligació de confidencialitat al seu personal ja sigui intern com extern, que estigui involucrat en l'execució del contracte i possibles subcontractistes i ha de controlar el seu compliment.

L'empresa adjudicatària ha de posar en coneixement de l'Agència, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de la informació.

3.14.2 Dades de caràcter personal

En relació amb el tractament de dades de caràcter personal, l'empresa adjudicatària del contracte basat donarà compliment com a encarregat de tractament del que estableix el Reglament General de Protecció de Dades.

3.14.3 Compliment del marc legal de ciberseguretat i del marc normatiu intern

L'empresa adjudicatària del contracte basat haurà de complir amb tots els requeriments que siguin d'aplicació d'acord amb el marc legal en matèria de ciberseguretat i amb el marc normatiu intern que siguin aplicables.

En relació al marc legal en matèria de ciberseguretat, i, en concret, al compliment de l'Esquema Nacional de Seguretat (ENS), l'empresa adjudicatària del contracte basat haurà d'assegurar la conformitat dels sistemes d'informació que sustentin la prestació de serveis o de les solucions que pugui proveir amb l'ENS durant tot el termini d'execució del contracte i, si escau, haurà d'estendre aquesta exigència a la cadena de subministrament. L'Agència de Ciberseguretat podrà requerir a l'empresa adjudicatària del contracte basat el lliurament de la documentació acreditativa de la conformitat amb l'ENS. L'empresa adjudicatària del contracte basat haurà de designar, segons estableix l'ENS, un punt de contacte per a la seguretat (POC) que canalitzarà i supervisarà el compliment dels requisits de seguretat de la informació i la gestió dels incidents que es puguin produir durant l'execució del contracte.

A més de l'ENS i la normativa i guies tècniques que el desenvolupen, l'empresa adjudicatària del contracte basat haurà de conèixer i aplicar el marc normatiu intern, que inclourà el Marc Normatiu de Seguretat la Informació de la Generalitat de Catalunya i la normativa pròpia, les directrius o instruccions de l'Agència de Ciberseguretat. Especialment haurà de complir amb la Política de seguretat aplicable i la normativa relativa a l'ús de les tecnologies de la informació i la comunicació, aprovada per Instrucció de la Secretaria d'Administració i Funció Pública i que es pot consultar al lloc

web d'aquesta Secretaria. Si escau, l'empresa adjudicatària del contracte basat haurà de desenvolupar els procediments que siguin necessaris per a poder aplicar el marc normatiu.

3.14.4 Capacitat tècnica

Per a poder executar el contracte i oferir garanties de la seva capacitat tècnica, l'empresa adjudicatària del contracte basat haurà de presentar compromís exprés d'adscripció al contracte dels mitjans personals que s'especifiquin als plecs, complint amb els requeriments definits de formació, i acreditar la disposició efectiva dels mateixos.

L'empresa adjudicatària del contracte basat ha de garantir que tot el personal sigui conscienciat, rebi formació i informació sobre els seus deures, obligacions i responsabilitats en matèria de seguretat derivats de la legislació, del marc normatiu intern i dels procediments i directrius aplicables i el seu deure de confidencialitat respecte a la informació a la que tingui accés.

3.14.5 Adquisició de productes/eines i productes o serveis de seguretat

Tant en el cas que es desenvolupin productes/eines, es facin integracions amb altres eines o s'adquireixin eines de mercat o qualsevol component de sistemes d'informació (hardware, software, etc.), aquests hauran de ser compatibles amb l'arquitectura de seguretat de l'Agència i complir amb els requeriments de seguretat que estableixi el marc legal i el marc normatiu intern, sotmetre's a proves tècniques de seguretat i aplicar les correccions necessàries prèviament a la posada en producció del producte/solució/eina. Caldrà incorporar el producte/eina dins el procés de desenvolupament segur de l'Agència de Ciberseguretat des de la fase de disseny fins a la posada en producció.

L'empresa adjudicatària del contracte basat haurà de garantir que disposa dels perfils amb la capacitació i la formació necessària per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició. A més, haurà de proporcionar formació i capacitació per al personal que designi l'Agència per tal que aquest personal adquireixi els coneixements necessaris per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició.

En cas que es contractin productes de seguretat o serveis de seguretat de les tecnologies de la informació i la comunicació que vagin a ser emprats en els sistemes d'informació de l'Agència, segons estableix l'ENS, hauran de tenir certificada la funcionalitat de seguretat relacionada amb el seu objecte d'adquisició. Els productes o serveis de seguretat hauran de constar al Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del Centre Criptològic Nacional o bé complir amb els criteris que estableixi l'Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centre Criptològic Nacional o, en el seu defecte, acreditar que el producte o servei disposa de requeriments equivalents.

3.14.6 Interconnexions

Segons preveu l'ENS, en el cas que sigui necessari realitzar interconnexions entre sistemes de l'empresa adjudicatària del contracte basat i l'Agència o amb d'altres entitats:

- No es podran dur a terme, tret que prèviament hagin estat autoritzades expressament per l'Agència.
- En cas que s'autoritzi una interconnexió, l'empresa adjudicatària del contracte basat haurà de garantir que es documentin com a mínim les característiques de la interfície, els requisits de seguretat i protecció de dades i la naturalesa de la informació intercanviada. Aquesta documentació l'haurà de facilitar a l'Agència.
- L'empresa adjudicatària del contracte basat haurà de participar en els mecanismes de coordinació que estableixi l'Agència i seguir els procediments establerts per aquest fi, per a

poder atribuir i exercir de manera efectiva, les responsabilitats en relació a cada sistema interconnectat.

3.14.7 Verificació del compliment i auditoria

L'Agència es reserva el dret a verificar i auditar, amb mitjans propis o de tercers, el compliment de les mesures de seguretat requerides en base al marc legal de ciberseguretat i al marc intern per als sistemes d'informació emprats per a l'execució del contracte, en el moment i amb la periodicitat que s'estimi convenient. L'Agència podrà requerir el seguiment dels plans d'acció derivats d'aquestes verificacions i auditories. L'empresa adjudicatària del contracte basat haurà de disposar dels recursos adients per a dur terme l'execució de les tasques que li corresponguin en relació a aquest model de compliment, donant resposta en els terminis marcats per l'Agència de Ciberseguretat. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'Agència de Ciberseguretat.

3.14.8 Incidents de seguretat

El POC haurà de notificar a l'Agència de Ciberseguretat qualsevol incident de seguretat que pugui redundar, directament o indirectament, en la seguretat dels sistemes d'informació, en els terminis i per les vies que determini o els procediments establerts. L'empresa adjudicatària del contracte basat haurà d'aportar tota la informació necessària per a la seva gestió i notificació als organismes competents per part de l'Agència de Ciberseguretat.

En cas que sigui necessari, l'empresa adjudicatària del contracte basat haurà de col·laborar amb qualsevol de les tasques que siguin requerides per part de l'Agència de Ciberseguretat per a la identificació, contenció, erradicació, recuperació i recopilació de les evidències dels incidents de seguretat.

3.14.9 Accés a la informació

L'empresa adjudicatària del contracte basat haurà de garantir l'accés del personal autoritzat de l'Agència de Ciberseguretat a la informació de seguretat (procediments, registre d'incidents, traces, etc.) per a poder desenvolupar l'objecte del contracte.

Tota la informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat. L'Agència de Ciberseguretat i l'empresa establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims.

3.15 Assegurament i control de la qualitat i la millora contínua

L'empresa ha de vetllar per l'excel·lència i millora contínua dels processos, components tècnics i serveis sota el seu abast.

Per tal de garantir que s'aborda la qualitat i la millora, l'adjudicatari haurà d'elaborar, mantenir i executar un "Pla de Qualitat i Millora Contínua" que inclogui, entre d'altres:

- Anàlisi i avaluació de les dades obtingudes de la mesura del servei, tant de producció i activitat com de gestió de l'incidental i operació.
- Plans de millora del servei orientats a millorar el compliment dels objectius del servei i del negoci.

- Accions per l'assegurament i control de la qualitat (revisions, proves, etc.), amb major rigor, intensitat i profunditat segons la criticitat del projecte/servei/component.
- Accions per reduir el nombre d'incidències, problemes freqüents i el suport.
- Accions per millorar la qualitat percebuda i la satisfacció dels usuaris.
- Accions preventives per la mitigació de riscos, tenint en compte la seva probabilitat i el seu impacte.
- Accions dirigides a millorar la gestió del coneixement i incrementar la usabilitat dels serveis.
- Accions per maximitzar l'eficiència i la sostenibilitat del servei.

3.16 Seguiment del servei

Les empreses adjudicatàries hauran de presentar un informe de seguiment de cada contracte basat d'acord amb els indicadors de compliment i altra informació rellevant pel seguiment del servei. Aquests informes s'avaluaran als comitès operatius i es formalitzaran i s'elevaran els seus resultats a la resta de comitès.

L'informe de seguiment haurà de tenir, com a mínim:

- Un informe de gestió dels serveis desenvolupats per a cada basat, amb indicació de les activitats realitzades i les previstes realitzar, les volumetries globals d'activitat i els indicadors de compliment especificats als. Acords de Nivell de Servei (ANS) de cada basat.
- Un informe de dedicació del basat a les diferents funcions requerides, per tal de poder avaluar la distribució dels esforços.
- Un informe d'accions de millora de l'activitat del propi basat, on es detallaran les accions de millora proposades amb informació rellevant per a la seva gestió (per exemple, el benefici previst obtenir, el termini d'implantació, etc.). Per cada millora implantada s'establirà, sempre que sigui possible, un indicador que s'afegirà a l'informe de gestió dels serveis. La periodicitat de l'informe de seguiment serà mensual, quant al seguiment de les activitats i la implantació de les millores. La presentació de les propostes de millora es farà amb la periodicitat indicada en cada contracte basat o el que es determini per part del responsable del contracte de l'Agència de Ciberseguretat.

Si existeix cap especificitat en aquest sentit, es recollirà al basat corresponent.

Pel control i seguiment del servei s'utilitzaran dades, mètriques i informes (en endavant informació) que serviran de suport als òrgans de gestió establerts i que són, en el seu conjunt, el mecanisme de seguiment i avaluació del servei. Aquesta informació es pot fer extensible a altres Unitats, Àrees, Direccions de l'Agència o tractar-se d'anàlisi puntual.

L'empresa adjudicatària del contracte basat és la responsable de generar i lliurar la informació que es determini en els diferents àmbits del servei, la qual ha de permetre a l'Agència governar, controlar i gestionar els serveis prestats objecte del contracte, tant des d'una òptica individual, com transversal i global.

La periodicitat, dates límit de lliurament, canals de transmissió, format exacte i contingut detallat de la informació a elaborar en tots els àmbits del servei, seran definits per l'Agència. L'Agència podrà sol·licitar, durant la vigència del contracte, ampliacions i canvis en el contingut, periodicitat, canals i format de la informació per ajustar-se a les necessitats de seguiment dels serveis.

L'empresa es compromet a automatitzar tot el possible els processos de generació i transmissió de la informació, arribant a la màxima integració possible.

L'empresa es compromet a proporcionar informació veraç i contrastada, i haurà de disposar dels mecanismes necessaris per garantir-ho. L'Agència podrà dur a terme les auditories que consideri necessàries per a la seva verificació, obligant-se l'empresa a participar-hi de manera activa i diligent sense cap cost afegit per a l'Agència.

L'Agència podrà sol·licitar informació de forma immediata i l'empresa hi donarà resposta ràpida fora de la planificació establerta.

3.17 Integració amb altres equips

L'adjudicatari del contracte basat haurà de portar a terme les activitats d'integració amb la resta d'equips operatius que conformen l'Agència, tant amb personal intern com amb personal d'altres empreses contractistes.

Aquesta integració s'haurà de portar a terme tant a nivell de la operativa diària (per garantir l'execució dels processos de la cadena de valor de l'Agència) com a nivell tàctic i operatiu.

Tot i això, els models de relació han de garantir els següents punts:

- Participació de l'adjudicatari en els processos que l'afectin.
- Compartició d'informació sobre fets puntuals (incidències, alertes, vulnerabilitats, etc.), ja sigui amb l'Agència com directament amb altres proveïdors.
- Compartició d'informació sobre fets agregats (tendències, patrons) i sobre afectacions col·lectives als diferents clients de l'Agència.
- Eliminació de les sitges organitzatives.
- Creació d'un fons comú de coneixement sobre la seguretat de la informació.
- Creació de bucles de retroalimentació que facilitin una resposta àgil davant de qualsevol nova situació en matèria de seguretat.